Separability and distillability in composite quantum systems – a primer –

M. Lewenstein[1], D. Bruß[1], J.I. Cirac[2], B. Kraus[2], M. Kuś[3], J. Samsonowicz[4], A. Sanpera[1] and R. Tarrach[5]

[1]*Institut für Theoretische Physik, Universität Hannover, D-30167 Hannover, Germany*
[2] *Institut ür Theoretische Physik, Universität Innsbruck, A–6020 Innsbruck, Austria*
[3] *Centrum Fizyki Teoretycznej, Polska Akademia Nauk, 02-668 Warsaw, Poland*
[4] *Department of Mathematics, Warsaw Technical University,00-661 Warsaw, Poland*
[5] *Departament d'Estructura i Constituients de la Materia, Universitat Barcelona, Spain*
(February 1, 2008)

Quantum mechanics is already 100 years old, but remains alive and full of challenging open problems. On one hand, the problems encountered at the frontiers of modern theoretical physics like Quantum Gravity, String Theories, etc. concern Quantum Theory, and are at the same time related to open problems of modern mathematics. But even within non-relativistic quantum mechanics itself there are fundamental unresolved problems that can be formulated in elementary terms. These problems are also related to challenging open questions of modern mathematics; linear algebra and functional analysis in particular. Two of these problems will be discussed in this article: a) the separability problem, i.e. the question when the state of a composite quantum system does not contain any quantum correlations or entanglement and b) the distillability problem, i.e. the question when the state of a composite quantum system can be transformed to an entangled pure state using local operations (local refers here to component subsystems of a given system).

Although many results concerning the above mentioned problems have been obtained (in particular in the last few years in the framework of Quantum Information Theory), both problems remain until now essentially open. We will present a primer on the current state of knowledge concerning these problems, and discuss the relation of these problems to one of the most challenging questions of linear algebra: the classification and characterization of positive operator maps.

I. INTRODUCTION

Quantum Mechanics celebrates in this year its first century of life. In October 1900, Max Planck presented to the "Deutsche Physikalische Gesellschaft" his seminal papers: "Über eine Verbesserung der Wienschen Spektralgleichung" and "Zur Theorie des Gesetzes der Energieverteilung im Normalspektrum" [1].

While there are no doubts about the success of Quantum Mechanics in explaining - beautifully - many of the problems concerning a variety of physical topics, it is worth stressing that Quantum Theory is by no means *passée*. It is nowadays still an open theory with several challenges which compel both Physics and Mathematics. Just a few years ago, it was common belief that the "really big" unsolved problems of theoretical physics pertained only to the domain of Quantum Gravity, that is the conjunction of Quantum Field Theory and General Relativity. Quantum Gravity and String Theory are closely related to unsolved challenges of modern mathematics, in particular concerning algebraic topology and algebraic geometry. However, to the surprise of many, the emerging field of Quantum Information Theory [2] has shown that even in the "simple" non-relativistic Quantum Theory there exist still fundamental open problems. The characterization of entanglement, and more specifically, the characterization of separability and distillability of quantum states are among these. Again, they are directly linked to unsolved challenges of mathematics concerning linear algebra and geometry, functional analysis and, in particular, the theory of C*-algebras [3].

In this paper we present some of these new open problems and report on the recent progress concerning them. The paper does not intend to be a review article on the subject of quantum entanglement, but rather an introduction – a primer – on the subject[1]. It contains nevertheless some new results: we present here two novel separability checks, and some new results concerning distillability of density matrices that possess a non-positive partial transpose. The presentation of these new results and their proofs require the introduction of some technical formalism. Therefore, they have been included as Appendices.

The paper is organized as follows: First, in Section II we explain what the entanglement problem means. In Section III we discuss the problem of separability, that is how to define and discriminate those states that contain only classical correlations and no quantum correlations. In Section IV we focus on the problem of distillability, that is, the possibility– by using local operations and classical communication only– to "distill" from a given ensemble of copies of a given mixed state a maximally entangled pure state. In that section we also present the current state-of-the-art. Finally, our summary remarks are contained in Section V.

---

[1]This paper has been presented by M. Lewenstein at the conference "Quantum Optics", Kühtai, January 2000.

II. THE ENTANGLEMENT PROBLEM

In order to explain what the entanglement problem means we first have to specify that in the following we will consider composite quantum systems [4]. Physical states of such systems are in general mixed and can be represented by density matrices, i.e. hermitian, positive definite linear operators of trace one, acting in the Hilbert space $\mathcal{H} = \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B} \otimes \ldots$, which is a tensor product of Hilbert spaces corresponding to subsystems $A, B, \ldots$ of the considered system.

Given a quantum state $\rho \in \mathcal{H}$, an apparently innocent question as *does this state contain quantum correlations?* will in general be very hard (if not impossible!) to answer. First of all, what does it mean that a quantum state does or does not contain quantum correlations? The answer seems to be straightforward: a system contains quantum correlations if the observables of the different subsystems are correlated, and their correlations cannot be reproduced by any means classically. That implies that some form of *non-locality* [4] is necessary in order to account for such correlations. For pure states – described by projections on a single vector acting on the Hilbert space $\mathcal{H}$ of the composite system – it is relatively easy to check if the correlations that they contain are classical, or not. For instance, it is enough to check if some kind of Bell inequality [5] is violated to assert that the state contains quantum correlations. In fact, there are many different "entanglement"- criteria and all of them reveal equivalent forms of the non-local character of the entangled pure states. For example, the demonstration that no local hidden variable (LHV) can account for the correlations between the observables in each subsystem is an equivalent definition of non-locality [6].

We know nowadays that these equivalences may fade away when one deals with mixed states. Contrary to a pure state, a mixed state can be prepared in many different ways. The fact that we cannot trace back how it was prepared prevents us from extracting all the information contained in the state. As a consequence, we lack (nowadays) general "entanglement" criteria that allow us to check if the correlations present in the system are genuinely quantum, or not. Despite the fact that many entanglement measures have been introduced, we do not know a "canonical" way of quantifying the entanglement [7]. Furthermore, different manifestations of non-locality are known to be not equivalent. For instance, Werner [6] introduced a family of mixed states that do not violate Bell-type inequalities (they admit a local hidden variable model), but nevertheless are non-local. The question whether there exists a violation of Bell inequalities in the, so-called, strong sense (where the observables take "unphysical" values) for all PPT entangled states (which we define below) remains open [8].

Therefore, the entanglement problem can be outlined as: *What does it mean that a given (mixed) state ρ contains or does not contain quantum correlations?*

III. THE SEPARABILITY PROBLEM

An essential step forward to understand what does entanglement mean is to discriminate first the states that contain classical correlations only (or no correlations at all). These states are termed separable states, and their mathematical characterization has been formulated by Werner [6]. We shall restrict ourselves here to the most simple composite systems: bipartite systems (with two subsystems traditionally denoted as Alice and Bob) of finite, but otherwise arbitrary dimensions. The states of bipartite systems are described by positive definite hermitian density matrices (with normalized trace) ρ, i.e. $\rho \geq 0$, $\rho = \rho^\dagger$ and $\mathrm{Tr}\rho = 1$. The density matrices act on the Hilbert space of the composite system $\mathcal{H} = \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$. Without loosing generality we will assume that dim $\mathcal{H}_A = M \geq 2$ and dim $\mathcal{H}_B = N \geq M$.

The most simple examples of separable states are just product states, i.e. $\rho = \rho^A \otimes \rho^B$ (ρ^A acts on $\mathcal{H}_A$, and ρ^B acts on $\mathcal{H}_B$). These states contain no correlations whatsoever. A straightforward extension of product states are the states that contain only classical correlations. Werner [6] provided us with the following operational definition of separability:

Definition 1 *A given state ρ is separable if and only if*

$$\rho = \sum_{i=1}^{k} p_i \rho_i^A \otimes \rho_i^B \ , \tag{1}$$

where $\sum_i p_i = 1$, and $p_i \geq 0$.

The above expression means that ρ can be written as a convex combination of product states. Equation (1) has a clear physical meaning. The state ρ can be prepared by Alice and Bob by means of local operations (unitary operations, measurements, etc.) and classical communication (LOCC). If ρ is separable the system does not contain quantum correlations. In spite of the definition, the characterization of such states is a rather arduous task. This is so among other facts because, in general, even for a given separable generic matrix we do not have an algorithm to decompose it according to Eq. (1). Thus, the separability problem, perhaps even more basic and fundamental than the entanglement problem can be formulated as: *Given a composite quantum state described by ρ, is it separable or not?*

Before proceeding further we introduce here the definitions that we shall use throughout the paper. Given a density matrix ρ, we denote by $K(\rho)$, $R(\rho)$, and $r(\rho)$ the kernel, the range and the rank of the matrix ρ defined as:

Definition 2 *Kernel $K(\rho) = \{|\phi\rangle : \rho|\phi\rangle = 0\}$.*

Definition 3 *Range $R(\rho) = \{|\phi\rangle : \exists |\psi\rangle : |\phi\rangle = \rho|\psi\rangle\}$.*

Definition 4 *Rank $r(\rho) = \dim R(\rho) = NM - \dim K(\rho)$.*

Let us introduce also the operation of "partial transposition" that will be used throughout the paper and is defined as:

Definition 5 *The partial transpose of ρ means the transpose only with respect to one of the subsystems. If we express ρ in Alice's and Bob's orthonormal product basis:*

$$\rho = \sum_{i,j}^{M} \sum_{k,l}^{N} \langle i, k |\rho| j, l\rangle |i, k\rangle\langle j, l|$$
$$= \sum_{i,j}^{M} \sum_{k,l}^{N} \langle i, k |\rho| j, l\rangle |i\rangle_A \langle j| \otimes |k\rangle_B \langle l|, \qquad (2)$$

then the partial transposition with respect to Alice is expressed as:

$$\rho^{T_A} = \sum_{i,j}^{M} \sum_{k,l}^{N} \langle i, k |\rho| j, l\rangle |j\rangle_A \langle i| \otimes |k\rangle_B \langle l|. \qquad (3)$$

Note that ρ^{T_A} is basis-dependent, but its spectrum is not. The partial transpose ρ^{T_A} may be ≥ 0, but does not have to be! As $(\rho^{T_A})^{T_B} = \rho^T$, and as $\rho^T \geq 0$ always holds, positivity of ρ^{T_A} implies positivity of ρ^{T_B} and vice versa.

A major step in the characterization of the separable states was done by Peres [9] and the Horodecki family [10]. Peres provided a "userfriendly" and very powerful necessary condition for separability. Later on, Horodecki's demonstrated that this condition is also sufficient for composite Hilbert spaces of dimension 2×2 and 2×3. Their results are enclosed in the following two theorems:

Theorem 1 *If ρ is separable then $\rho^{T_A} \geq 0$.*

A matrix that verifies the above theorem is termed "PPT" for positive partial transpose. Notice that being a PPT state is a necessary condition for separability.

Theorem 2 *If $\rho^{T_A} \geq 0$ in spaces of dimensions 2×2 or 2×3 then ρ is separable.*

In general, there exist PPT states ρ (i.e. states with $\rho^{T_A} \geq 0$) which are not separable in $M \times N$ spaces ($M = 2, N \geq 4$ or $M \geq 3$) [11]. The PPT entangled states have been termed "bound entangled states" to distinguish them from the "free entangled states". This latter names are associated with the distillability property, which we will discuss in the later sections of this paper. "Bound entangled states" are entangled, however, no matter how many copies of them we have, these

states cannot be "distilled" via local operations and classical communication to the form of a pure entangled state [12]. We encounter thus new problems such as: *How can one distinguish a separable state ρ from a PPT state ρ? Are all non-PPT states (NPPT states) "free entangled" i.e. distillable?* But before trying to answer these questions (that will bring us directly to the problem of distillability), we will first present a physical explanation of what separability means, and discuss shortly the recent progress concerning the quest for separability criteria.

A. Physical interpretation of separability

Let us now interpret the condition of positive partial transposition from a physical point of view. We start by considering symmetry transformations in the Hilbert space of each subsystem. Wigner's theorem [13] tells us that every symmetry transformation is necessarily implemented by a unitary (U) or anti-unitary (A) matrix. The tensor product of a unitary and an anti-unitary transformation $U_A \otimes A_B$ (or $A_A \otimes U_B$) results in a transformation which is neither unitary, nor anti-unitary in $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, and whose action on a general ket of the composite system $|\psi\rangle \in \mathcal{H}$, furthermore, cannot be properly defined. However, its action on a product ket $|e, f\rangle \equiv |e\rangle \otimes |f\rangle$, (where $|e\rangle \in \mathcal{H}_A$ and $|f\rangle \in \mathcal{H}_B$) is, apart from a phase ambiguity, well defined. Thus, the action of a combined transformation of the type $U_A \otimes A_B$ on projectors corresponding to pure product states is well defined without any ambiguity. As a separable state ρ_s can always be rewritten as a statistical mixture of product vectors (see Def. 1) it is clear that under the combined transformation $U_A \otimes A_B$ (or $A_A \otimes U_B$), ρ_s transforms into:

$$\rho_s \to \rho_s' = \sum_{i=1}^{k} p_i \left(|e_i'\rangle\langle e_i'| \otimes |f_i'\rangle\langle f_i'| \right) \qquad (4)$$

where $|e_i'\rangle \equiv U_A |e_i\rangle \in \mathcal{H}_A$; $|f_i'\rangle \equiv A_B |f_i\rangle \in \mathcal{H}_B$. Therefore, ρ_s' describes also a physical state so that ρ_s' is a positive definite hermitian matrix (with normalized trace). This is what characterizes separable states: that any local symmetry transformation, which obviously transforms local (in this context local refers to each of the subsystems) physical states into local physical states, also transforms the composite global state into another physical state.

There exists only one independent anti-unitary symmetry [13], and its physical meaning is well known: time reversal. Any other anti-unitary transformation can be expressed in terms of time reversal (as the product of a unitary matrix times time reversal). Thus separability of composite systems implies the lack of correlation between the time arrows of their subsystem. In other words: given a separable composite state, reversing time

in one of its subsystems leads again to a physical state [14,15].

B. Quest for separability criteria and checks

In the recent years there has been a growing effort in searching for necessary and sufficient separability criteria and checks. Several necessary conditions for separability are known: Werner has derived a condition based on the analysis of local hidden variables (LHV) models and the mean value of the, so-called, flipping operator [6], the Horodecki's have proposed a necessary criterion based on the so-called α-entropy inequalities [16], etc... Quite recently, a general and sufficient condition for separability was discovered by the Horodecki family in terms of positive maps. A map is defined positive if it maps positive operators into positive operators. The condition found by the Horodecki's, states that ρ is separable iff the tensor product of any positive map acting on one subsystem A and the identity acting on other subsystem B maps ρ into a non-negative operator. This definition, however, involves the characterization of the set of all positive maps which is *per se* a major task. Later on the reduction criterion of separability was introduced [17,18]:

Criterium 1 *If ρ is separable then the map $(\Gamma_A \otimes \mathbb{1})$: $\rho \to (\mathbb{1}_A \otimes \text{Tr}_A \rho) - \rho$ must be positive.*

Violation of this criterion is sufficient for entanglement to be free. Following the reduction criterion, a simple and still quite powerful sufficient condition for distillability was provided in Ref. [19], where P. Horodecki *et al.* showed that if the rank of at least one of the reduced density matrices $\rho_A = \text{Tr}_B \rho$ and $\rho_B = \text{Tr}_A \rho$ exceeds the rank of ρ, then ρ is distillable, *ergo* is non-separable and NPPT. In particular, it was concluded in Ref. [19] that there is no bound entanglement of rank 2.

Sufficient conditions for separability are also known. In Ref. [20] it was proven that any state close enough to the completely random state $\pi = I/NM$ is separable. In [20] there were also given the first quantitative bounds for the radius of the ball surrounding π that does not contain any entangled state. Much better bounds were found in the following works [21], where it was proven that a full rank mixed state is separable provided that its smallest eigenvalue is greater or equal to $(2 + MN)^{-1}$.

In Ref. [11], in which the first explicit examples of entangled states with PPT property were provided, another necessary criterion of separability was formulated. According to this criterion:

Criterium 2 *If the state ρ acting on a finite dimensional Hilbert space is separable then there must exist a set of product vectors $\{|e_i, f_i\rangle\}$ that spans the range $R(\rho)$*

such that the set of partially complex conjugated product states $\{|e_i^*, f_i\rangle\}$ spans the range of ρ^{T_A}.

The analysis of the range of the density matrices, initiated by P. Horodecki, turned out to be very fruitful, leading, in particular, to the algorithm of optimal decomposition of mixed states into the separable and inseparable part [22,23], and to systematic methods of constructing examples of PPT entangled states with no product vectors in their range, using either so-called unextendible product bases (UPB's) [24,25], or the method described in [26].

In the Appendices A and B we present two novel separability criteria and checks. One provides a necessary condition for separability, or rather a sufficient condition for entanglement. It detects the non-separability of the UPB states. The other criterion, or rather separability check, detects all separable states that are the convex combinations of two product states.

C. Recent progress in the separability problem

Despite many efforts and seminal results obtained in the recent years, the problem of separability remains essentially open. Recently, a considerable progress of in the study of PPT entangled states has been made [27,28]. The results obtained allow us to hope to develop a systematic way of constructing optimal criteria for separability in arbitrary Hilbert spaces [29].

Our method employs the idea of "subtracting projectors on product vectors" [22,23]: if there exists a product vector $|e, f\rangle \in R(\rho)$ such that $|e^*, f\rangle \in R(\rho^{T_A})$, the projector onto this vector (multiplied by some $\lambda > 0$) can be subtracted from ρ, such that the remainder is positive definite and PPT. Our results can be divided into three groups.

First, we have studied and found separability criteria for density matrices of sufficiently low dimensional rank. Also constructive algorithms to decompose optimally (with the smallest possible number of terms) the separable matrix according to Eq. (1) - i.e. in product states - have been provided for low rank matrices. For the general case of composite systems with the Hilbert space $\mathcal{H}^{\mathcal{M}} \otimes \mathcal{H}^{\mathcal{N}}$ ($M \leq N$) our findings are essentially contained in the following two theorems:

Theorem 3 *If ρ is PPT such that $r(\rho) = k \leq N$ and ρ cannot be embedded in a $2 \times (k-1)$ dimensional space then ρ is separable.*

In particular when ρ has rank N there exist typically exactly N product vectors $|e_i, f_i\rangle$ in the range of ρ such that $|e_i^*, f_i\rangle \in R(\rho^{T_A})$; ρ is then a convex combination of projections onto these vectors.

Theorem 4 *If* $r(\rho) + r(\rho^{T_A}) \leq 2NM - N - M + 2$ *then typically there exists a* **finite** *number of product vectors* $|e, f\rangle \in R(\rho)$ *such that* $|e^\star, f\rangle \in R(\rho^{T_A})$.

These product vectors are the only possible candidates to appear in the decomposition of Eq. (1). Finding them requires solving a system of polynomial equations. After these equations are solved, one can check whether ρ has the decomposition (1). The problem is infinitely easier than the original one since we know now all possible projectors that can be used, and we know that their number is finite. In fact, checking in such a situation whether ρ is separable or not can be done in a finite number of computational steps!

Second, we have studied the structure and generic form of low rank PPT entangled matrices. To study low rank PPT entangled matrices has a twofold purpose. On one hand, the complexity of the problem is reduced, and therefore it is possible to find separability criteria. But, perhaps the most important is the fact that, given a density matrix ρ, one can always decompose it as :

$$\rho = \Lambda \rho_{sep} + (1 - \Lambda)\delta\rho \, , \qquad (5)$$
$$\rho^{T_A} = \Lambda {\rho^{T_A}}_{sep} + (1 - \Lambda)\delta\rho^{T_A} \, , \qquad (6)$$

where $\rho_{sep} = \sum_i \Lambda_i P_i$ is a separable state, P_i are projectors onto product states and Λ is maximal. All the information concerning entanglement is then contained in the remainder $\delta\rho$ ($\delta\rho^{T_A}$) which has low rank and can be termed as a "pure" PPT entangled state, or "edge" PPT entangled state. This state has a property that no projection onto the product state can be subtracted from it, keeping the rest positive definite and PPT. Formally, there exist no product vectors $|e, f\rangle \in R(\delta\rho)$ such that $|e^*, f\rangle \in R(\delta\rho^{T_A})$. The "edge" states violate in the extremal sense the Criterion of Ref. [11]. The problem of the separability reduces now to the problem of separability of the "edge" states, and to the question whether a given mixture of an "edge" and a separable state is separable or not.

In other words, any matrix ρ can be decomposed in a separable part (that contains product vectors in the range) and a remainder, which is the "edge" state. $\delta\rho$ and $\delta\rho^{T_A}$ are low rank matrices that contain all the information related to entanglement. Obviously, knowing the structure of those matrices is therefore of capital importance.

Finally, let us mention a different approach to the entanglement problem, that is based on the so-called entanglement witnesses. An entanglement witness is an observable E that reveals the entanglement of an entangled density matrix ρ. B. Terhal [8,25] introduced entanglement witnesses through the following theorem:

Theorem 5 *If* ρ *is entangled then there exists an entanglement witness* E *such that*

$$\mathrm{Tr}(E\rho_{sep}) \geq 0, \qquad (7)$$
$$\mathrm{Tr}(E\rho) < 0 \qquad (8)$$

for all separable matrices ρ_{sep}.

Entanglement witnesses represent – in some sense – a kind of Bell inequality which is violated by the entangled state ρ. Each entanglement witness E on an $M \times N$ space defines a positive map $\mathcal{E}$ that transforms positive operators on an M or N–dimensional Hilbert space into positive operators on an M or N–dimensional space [31]. The maps corresponding to entanglement witnesses are positive, but not completely positive, and in particular their extension to $M \times N$ spaces allows to "detect" the entanglement of ρ. The maps corresponding to entanglement witnesses for PPT states are, moreover, non decomposable: they cannot be represented as a combination of completely positive maps and partial transposition.

For every "edge" state it is possible to construct an entanglement witness [29] as:

$$E = P_{K(\rho)} + (P_{K(\rho^{T_A})})^{T_A} - \epsilon, \qquad (9)$$

where $P_{K(\rho)}$, $P_{K(\rho^{T_A})}$ are projections onto the kernel of ρ and the kernel of ρ^{T_A}, and $0 < \epsilon = \min\langle e, f| P_{K(\rho)} + (P_{K(\rho^{T_A})})^{T_A} |e, f\rangle$, where the minimum is taken over all possible product vectors.

We have not only been able to find entanglement witnesses, and the corresponding non–decomposable positive maps for arbitrary "pure" or "edge" PPT states, but also to optimize them in a certain sense [29]. Optimized entanglement witnesses detect significantly more entangled PPT states than the non–optimized ones.

We hope very much that these studies will allow us to characterize extremal points in the convex set of PPT entangled matrices, and then to characterize the extremal points in the convex set of positive maps [30]. If this program is realized, the separability problem will be solved. So far, however, only the first steps have been done and the problem remains open and challenging.

IV. THE DISTILLABILITY PROBLEM

On having said that, we shall attack now the related problem of the distillability of mixed quantum states. For many applications in quantum information processing [32] and communication one needs a maximally entangled state, that is, a state which in $M \times N$ dimensional space can be brought by a local change of basis to the form

$$|\Psi_{max}\rangle = \frac{1}{\sqrt{M}} \sum_{i=1}^{M} |i, i\rangle, \qquad (10)$$

which is shared between two parties.

Although in principle one can create pure and maximally entangled states, in realistic situations any pure state will evolve to a mixed state due to its interaction with the environment. A standard example concerns a situation when two entangled particles (photons, atoms,...) representing the two subsystems are sent from the source to the two involved parties, Alice and Bob, through noisy channels. In order to overcome the noise created during the transmission, the idea of distillation and purification, i.e. enhancement of the given non-maximal mixed entanglement by local operations and classical communication (LOCC) was proposed by Bennett *et al.* [33], Deutsch *el al* [34] and Gisin [35]. Again, for Hilbert spaces of composite systems of dimension lower or equal to 6, any mixed entangled state can always be distilled to its pure form. Since for such systems entanglement is equivalent to the NPPT property, we conclude that for 2×2, and for 2×3 systems, all NPPT states are distillable [36]. However, it was shown by Horodecki family [12] that in higher dimensions there exist states (namely PPT entangled states), termed as bound entangled states, which cannot be distilled, in contraposition to free entangled states [37]. The distillability problem can be formulated as: *Given a density matrix ρ, is it or is it not distillable?*

Let us now define the distillability property, first on an intuitive, and then on a more formal basis.

Definition 6 *ρ is distillabe if by performing LOCC on some number K of copies ρ, Alice and Bob can distill a state arbitrary close to $|\Psi_{max}\rangle$, i.e.*

$$\rho \otimes .... \otimes \rho \longrightarrow |\Psi_{max}\rangle \langle \Psi_{max}|. \qquad (11)$$

The above definition is not very precise – it requires to specify what the LOCC can do with K copies of ρ, and does not give any practical advice about how to answer the question of distillability. Fortunately we can use the theorem of Ref. [12], which states that instead of studying the whole set of possible LOCC, in order to determine the distillability of a given density matrix it is sufficient to study projections on a 2×2 dimensional subspace of the Hilbert space in which ρ acts. The theorem is very useful since it reduces the problem of distillability to a very precisely stated mathematical question; in fact from now on we will use it as a definition of distillability.

Theorem 6 *ρ is distillable iff there exists a number of copies K, and a projector $P_{2\times2}$ onto a 2×2-dimensional space spanned by:*

$$|e_i\rangle \in \underbrace{\mathcal{H}_\mathcal{A} \otimes ... \otimes \mathcal{H}_\mathcal{A}}_{K-times} , \ i = 1, 2, \qquad (12)$$

$$|f_i\rangle \in \underbrace{\mathcal{H}_\mathcal{B} \otimes ... \otimes \mathcal{H}_\mathcal{B}}_{K-times} , \ i = 1, 2, \qquad (13)$$

such that the projection

$$\sigma = P_{2\times2}\rho^{\otimes K}P_{2\times2}, \qquad (14)$$

is NPPT (i.e. is distillable).

An alternative way of formulating the above theorem is the following: ρ is distillable iff there exists a state $|\psi\rangle$ from a 2×2-dimensional subspace,

$$|\psi\rangle = a|e_1^\star\rangle|f_1\rangle + b|e_2^\star\rangle|f_2\rangle , \qquad (15)$$

such that $\langle\psi|(\rho^{T_A})^{\otimes K}|\psi\rangle < 0$ for some K.

The idea of the proof of the above theorem is the following: if ρ is distillable it means that one can produce a maximally entangled state, and it is then easy to project (using local projections) that state onto a pure state in a 2×2-dimensional subspace. On the other hand, if there is a $|\psi\rangle$ as in equation (15), such that $\langle\psi|\rho^{T_A}|\psi\rangle < 0$, then one can first project onto the 2×2 subspace to which $|\psi\rangle$ belongs. This is a 2×2 subspace in which the projected matrix is NPPT, *ergo* it is distillable. We can then distill several maximally entangled state in this subspace, rotate them unitarily and locally, and combine to a maximally entangled state in the whole space.

Let us now ask what does the criterion of partial transposition,– which plays an important role in the separability problem as we have seen before–, tell us about the distillability problem?

Theorem 7 *If $\rho^{T_A} \geq 0$ (ρ is PPT) then ρ is not distillable [12].*

Theorem 8 *If $\rho^{T_A} \ngeq 0$ (ρ is NPPT) in dimensions 2×2, 2×3 then ρ is distillable [36].*

The later holds also for $2 \times N$ systems, see [38].

A. Recent progress in the distillability problem

At the end of the last section we have seen that every density matrix with a positive partial transpose cannot be distilled, and that for low dimensions the converse is true. In this section we want to discuss the conjecture that in higher dimensions there are states with a non-positive partial transpose, which are however non-distillable [38,39]. In other words, non-positivity of the partial transpose seems to be a *necessary*, but not a *sufficient* condition for distillability.

The states which are believed to be non-distillable [38], belong to a one-parameter family, which lives in dimension $N \times N$:

$$\rho(\alpha) = \frac{1}{m(\alpha)}(P_S + \alpha P_A) \text{ with } \alpha \geq 0 , \qquad (16)$$

where P_S and P_A denote projectors onto the symmetric and antisymmetric subspace, respectively, and m is some normalization. This family is generic in the sense that *every* density matrix in $N \times N$ can be depolarised locally to a state from our family. In this sense these states are nothing more but Werner states [6] defined for $N \times N$ systems.

The partial transpose of $\rho(\alpha)$ is given by

$$\rho^{T_A}(\alpha) = \frac{1}{n(\beta)}(1 - \beta P) , \qquad (17)$$

where $n(\beta)$ is the normalization, P is the projector onto a maximally entangled state $|\Psi_{max}\rangle = \sum_{i=1}^{N} |ii\rangle / \sqrt{N}$, and the relation between α and β is:

$$\beta = \frac{N(\alpha - 1)}{\alpha + 1} \quad \text{with} \; -N \leq \beta \leq N . \qquad (18)$$

Note that for $\beta \leq 1$ the matrix ρ^{T_A} is positive definite , i.e. ρ is PPT and thus is not distillable. For $\beta > 1$ one finds that ρ^{T_A} is not positive definite, i.e. ρ is NPPT and the question of distillability is open.

The nice thing about the considered family of states is that if we show that:
(i) ρ is distillable for all $\beta > 1$, then all ρ with NPPT are distillable, because all ρ can be reduced to the "canonical" form (16).
(ii) if there exists $\beta \leq N$, such that ρ is NPTT and is not distillable, then not all ρ with NPPT are distillable. In other words there exist undistillable ρ's with NPPT. Both alternatives (if proven) would be an extremely important result. At the moment it seems that the second alternative is true [38,39], but strictly speaking the problem is open. We shall see below that ρ is distillable for $\beta > 3/2$, so that in fact interesting region of the parameter β lies between 1 and 3/2.

Before presenting some partial results on the way to the complete proof, which is yet unknown, let us introduce the concept of K-distillability, by which we define distillability with respect to K copies.

Definition 7 ρ *is K-distillable iff there* $\exists \,| \psi \rangle$ *as given in Eq. (15) such that*

$$\langle \psi \,|(\rho^{T_A})^{\otimes K}| \psi \rangle < 0. \qquad (19)$$

The basic theorem that we have proven so far determined the region of the parameter β for which the matrix ρ of Eq. (16) is not K-distillable. Our results hold for arbitrary $N \times N$ systems, but here we specify them to case of two qutrit systems (3×3).

Theorem 9 *Let* $\rho \sim P_S + \alpha P_A$, *i.e.* $\rho^{T_A} \sim 1 - \beta P$ *act in 3×3 space, then:*

- ρ *is not 1-distillable for* $1 \leq \beta \leq \frac{3}{2}$;

- ρ *is not 2-distillable for* $1 \leq \beta \leq \frac{5}{4}$;

- ρ *is K-undistillable for* $1 \leq \beta \leq \beta_K$, *where the best bound for β_K obtained so far is:*

$$\beta_K \sim 1 + \frac{1}{3^{K/3}K^{1/3}}. \qquad (20)$$

As we see, for every K there exist a region of β (see Fig.1) in which ρ is not distillable. Unfortunately, this region shrinks, however to a point, as K goes to infinity. If we have an arbitrary number of copies of ρ we cannot say whether we will be able or not to distill it. The proof of the above theorem is technical, but essentially simple. Below we sketch the proof concerning 1– and 2–distillability

B. 1–Distillability

Let $Q = 1 - P$ be the projector complementary to P, where P is the projector onto maximally entangled states. For one copy of the matrix ρ we have that for any $| \psi \rangle$ given by Eq. (15):

$$\langle \psi \,|Q - \beta P| \psi \rangle = \langle \psi \,|1 - (1 + \beta)P| \psi \rangle \geq$$
$$1 - (1 + \beta)\frac{2}{3} \geq 0 \qquad (21)$$

for $\beta \leq \frac{3}{2}$. The last inequality follows from the fact that the projection $|\langle \psi |\Psi_{max}\rangle|^2$ of an arbitrary vector living in a 2×2 subspace onto a maximally entangled vector in 3×3 space must not be greater than 2/3. The above considerations imply also that for $\beta > 3/2$ the matrix is 1–distillable, because there exists a vector in a 2×2 subspace for which $|\langle \psi |\Psi_{max}\rangle|^2 = 2/3$. This proves that ρ is distillable for $\beta > 3/2$.

C. 2–Distillability

To show that 2 copies of ρ cannot be distilled for some interval of β, we first observe that Q is separable, i.e.

$$Q = \sum_{i}^{R} p_i | e_i, f_i \rangle \langle e_i, f_i |. \qquad (22)$$

Denoting by Tr_i the trace over the i–th copy, and by Q_i – the projector Q for the i–th copy we get

$$\text{Tr}(\langle \psi \,|Q_1| \psi \rangle) = \sum_{i=1}^{R} p_i \langle \psi| e_i, f_i \rangle \langle e_i, f_i| \psi \rangle \qquad (23)$$

where $| \psi \rangle_i = \langle \psi| e_i, f_i \rangle$ is a vector in the second copy space with 2 Schmidt coefficients, i.e. of the form (15). Similar result holds for the second copy. Then, using the results for 1–distillability we obtain

$$\langle\psi\,|Q\otimes(Q-\frac{1}{2}P)|\,\psi\rangle\geq 0, \tag{24}$$

$$\langle\psi\,|(Q-\frac{1}{2}P)\otimes Q|\,\psi\rangle\geq 0. \tag{25}$$

Now, by adding the above results and dividing by two we obtain

$$\langle\psi\,|(Q-\frac{1}{4}P)\otimes(Q-\frac{1}{4}P)|\,\psi\rangle\geq\langle\psi\,|\frac{1}{16}P\otimes P)|\,\psi\rangle\geq 0, \tag{26}$$

so that we see that ρ is not 2–distillable for $\beta\leq 5/4$.

D. Distillability in general

In the Ref. [38] we have performed extensive numerical studies and looked for the minimum of $\langle\psi\,|(\rho^{T_A}(\beta))^{\otimes K}|\,\psi\rangle$ over all possible $|\,\psi\rangle$ of the form (15). The numerical results indicate clearly that:

- ρ is not 2-distillable for $1\leq\beta\leq\frac{3}{2}$;

- ρ is not 3-distillable for $1\leq\beta\leq\frac{3}{2}$.

It is a challenging and open problem to understand these results. So far we have only achieved some progress in the problem of 2–distillability. We have proven that the states $|\,\psi\rangle$ for which $\langle\psi\,|(\rho^{T_A}(\beta))^{\otimes K}|\,\psi\rangle=0$, and which (as we know) provide the global minimum of $\langle\psi\,|(\rho^{T_A}(\beta))^{\otimes K}|\,\psi\rangle$ for $\beta\leq 5/4$, provide also a local minimum of $\langle\psi\,|(\rho^{T_A}(\beta))^{\otimes K}|\,\psi\rangle$ equal to zero for $3/2\geq\beta>5/4$. The proof of this fact is presented in the appendix C. There exists a well-based suspicion that ρ is not distillable in the entire region of $1\leq\beta\leq 3/2$.

V. CONCLUSIONS

There is only one conclusion of this paper: Quantum Theory is an open and challenging area of physics. It offers still fundamental and fascinating problems that can be formulated at elementary level, and yet they are related to challenges of the modern mathematics. Particular examples of those are separability and distillability of composite quantum systems.
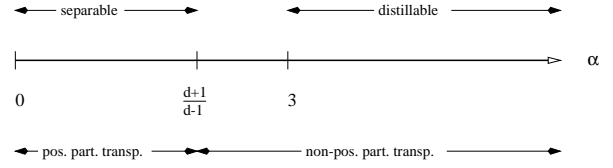
FIG. 1. Separability and distillability properties of ρ in arbitrary $d\times d$ dimensional space. In the region between separable and distillable ρ is NPPT and most presumably non-distillable.

APPENDIX A: SUFFICIENT CRITERION FOR INSEPARABILITY

Our sufficient criterion of inseparability (i.e. a necessary criterion for separability) is based on the following Lemma. Let us assume the product vectors $|e,f\rangle$ to be normalized.

Lemma 1 If $\quad max\{\mathrm{Tr}(\rho^2),\mathrm{Tr}((\rho^{T_B})^2),\mathrm{Tr}(\rho\rho^{T_B})\}\quad>$ $max_{|e,f\rangle}\langle e,f|\rho|e,f\rangle$, then ρ is inseparable.

Let us prove that this statement is true in the case where $\{\mathrm{Tr}(\rho^2)=\max\{\mathrm{Tr}(\rho^2),\mathrm{Tr}((\rho^{T_B})^2),\mathrm{Tr}(\rho\rho^{T_B})\}$. All the other cases can be proved in the same way which implies that we can take the maximum of those three values.
Proof: We define $r=\max_{|e,f\rangle}\langle e,f|\rho|e,f\rangle$ and the witness, $X=1-\frac{1}{r}\rho$. Assuming that $\mathrm{Tr}(\rho)=1$ we have that $\mathrm{Tr}(X\rho)<0$. It remains to prove that $\mathrm{Tr}(X\tilde\rho)>0$ for all $\tilde\rho$ separable. We write $\tilde\rho=\sum_i\lambda_i|e_i,f_i\rangle\langle e_i,f_i|$, and observe that: $r\mathrm{Tr}(X\tilde\rho)=\mathrm{Tr}[(\max_{|e,f\rangle}\langle e,f|\rho|e,f\rangle-\rho)\tilde\rho]=$ $\sum_i\lambda_i(\max_{|e,f\rangle}\langle e,f|\rho|e,f\rangle-\langle e_i,f_i|\rho|e_i,f_i\rangle)\geq 0$.

Unfortunately this criterion does not work for the Horodecki PPT states in 2×4 space [11]. It does, however, detect the entanglement of the PPT states constructed from UPB's [24]. In such case $\rho=P/K$, where P is a projector onto a space that does not contain any product vectors, $K=r(P)$, and $P=P^{T_B}$. Our criterion gives $\mathrm{Tr}(\rho^2)=\mathrm{Tr}((\rho^{T_B})^2)=\mathrm{Tr}(\rho\rho^{T_B})=1/K$, while $\langle e,f|\rho|e,f\rangle=\langle e,f|P|e,f\rangle/K<1/K$.

APPENDIX B: SEPARABILITY CHECK FOR BINARY MIXTURES OF PRODUCT STATES

If a separable matrix is a mixture of two product states (here we call such matrix a binary mixture), then it is relatively easy to check separability. Assume ρ of the following form:

$$\rho=\sum_{i=1}^{K}p_i\rho_i^A\otimes\rho_i^B, \tag{B1}$$

where all $p_i > 0$, and $\sum_i p_i = 1$. Let μ and ν be density matrices acting in Alice and Bob's space respectively. Let us define the matrix function

$$M(\mu, \nu) = \sum_{i=1}^{K} p_i (\rho_i^A - \mu) \otimes (\rho_i^B - \nu). \qquad (B2)$$

Interestingly, M can be calculated without the explicit use of the representation (B1),

$$M(\mu, \nu) = \rho - \mu \otimes \rho_B - \rho_A \otimes \nu + \mu \otimes \nu, \qquad (B3)$$

where the reduced density matrices are $\rho_{A,B} = \mathrm{Tr}_{B,A}\rho$.

For $K = 2$ we have an obvious Lemma:

Lemma 2 *If ρ is a mixture of two product states (with $p_1 = p, p_2 = 1 - p$) then the equation $M(\mu, \nu) = 0$ has at least two solutions $\mu = \rho_1^A$, $\nu = \rho_2^B$, and $\mu = \rho_2^A$, $\nu = \rho_1^B$.*

The "opposite" implication is also true.

Lemma 3 *If the equation $M(\mu, \nu) = 0$ has solutions such that $\mu \geq 0$, $\mu = \mu^\dagger$, $\mathrm{Tr}\mu = 1$, $\nu \geq 0$, $\nu = \nu^\dagger$, $\mathrm{Tr}\nu = 1$, then ρ is either a separable binary mixture, or a nonseparable binary pseudomixture.*

The proof follows directly from Eq. (B3). ρ can be written as

$$\rho = \mu \otimes (\rho_B - (1-p)\nu) + (\rho_A - p\mu) \otimes \nu, \qquad (B4)$$

with some $0 \leq p \leq 1$. We immediately see that ρ is separable if there exists $p \in [0,1]$ such that $\rho_B - (1-p)\nu \geq 0$ and $\rho_A - p\mu \geq 0$. This implies that the ranges $R(\mu)$ and $R(\nu)$ must be included in the ranges of ρ_A, and ρ_B, respectively; at the same time p must fulfill the conditions $p\|\mu(\rho_A)^{-1}\| \leq 1$, and $(1-p)\|\mu(\rho_B)^{-1}\| \leq 1$, where $\|.\|$ denotes the operator norm (for details see [27]).

Checking if the equation $M(\mu, \nu) = 0$ has solutions is very easy. We can use a product basis $\{O_i^A \otimes O_j^B\}_{i=1,\ldots,M^2; j=1,\ldots,N^2}$ in the operator space. Such basis can be chosen to be orthonormal and hermitian with respect to the trace scalar product. The equation $M(\mu, \nu) = 0$ projected onto the ij–th element of the basis reads:

$$\rho_{ij} - \mu_i \rho_{Bj} - \rho_{Ai}\nu_j + \mu_i \nu_j = 0. \qquad (B5)$$

where $\rho_{ij} = \mathrm{Tr}\rho O_i^A \otimes O_j^B$, $\rho_{Ai} = \mathrm{Tr}\rho_A O_i^A$, $\rho_{Bj} = \mathrm{Tr}\rho_B O_j^A$, etc...We have thus $N^2 M^2$ such equations for $M^2 + N^2$ real coefficients μ_i, ν_j. The equations have a very simple structure and therefore it is easy to check: a) if they have a solution; b) if the resulting μ and ν are positive definite; c) if there exists p such that both terms on the RHS of Eq. (B4) are positive definite.

The above formulated separability check can be easily generalized to systems of R parties and separable mixtures of R product states for $R > 2$.

In this appendix we will find the states that lead to a local minimum for projection onto a two-dimensional subspace as in equation (19) in the case of 2 copies (in dimension 3×3), for the critical value of the parameter $\beta = 3/2$.

We will proceed as follows: our problem will be formulated in terms of a function $f(\lambda, \psi)$ that has to be minimized with respect to ψ. We will find a family of states ψ for which f is shown to reach a local minimum, for a range of parameters λ.

We introduce a parameter λ and will study the following function:

$$f(\lambda, \psi) = \frac{1}{M^2} \langle \psi | (1 + |1 - 2\lambda|) \mathbb{1} \otimes \mathbb{1} + \frac{9}{4} P \otimes P$$
$$- 3(\lambda \cdot \mathbb{1} \otimes P + (1-\lambda)P \otimes \mathbb{1})| \psi \rangle$$
$$= \langle \psi | \rho_2(\lambda)| \psi \rangle, \qquad (C1)$$

where the last line defines $\rho_2(\lambda)$, and P is the projector onto a maximally entangled state. Here λ is a given fixed parameter with $0 < \lambda < 1$. The case $\lambda = \frac{1}{2}$ corresponds to ρ_2 being the partial transpose of two copies of $\mathbb{1} - 3P/2$. In the notation of Section IV this corresponds to the value of $\beta = 3/2$. We are looking for the minimum of f with respect to $| \psi \rangle$. This state lives in the two-dimensional subspace and can be written in the Schmidt decomposition (cf. [4])

$$| \psi \rangle = a| e_1 \rangle_A | f_1 \rangle_B + b| e_2 \rangle_A | f_2 \rangle_B, \qquad (C2)$$

where the states $| e_i \rangle, | f_i \rangle$ are normalised and $\langle e_1^* | e_2 \rangle = 0 = \langle f_1^* | f_2 \rangle$ and $| a |^2 + | b |^2 = 1$. For clarity we kept the indices A and B.

Let us rewrite the terms in equation (C1), sorting them not pairwise, but with respect to Alice and Bob:

$$\mathbb{1} \otimes \mathbb{1} = \sum_{i,j,r,s=1}^{3} | ir \rangle_A | js \rangle_B \langle ir |_A \langle js |_B,$$

$$P \otimes P = \frac{1}{9} \sum_{i,j,r,s=1}^{3} | ir \rangle_A | ir \rangle_B \langle js |_A \langle js |_B,$$

$$P \otimes \mathbb{1} = \frac{1}{3} \sum_{i,j,r,s=1}^{3} | ir \rangle_A | is \rangle_B \langle jr |_A \langle js |_B,$$

$$\mathbb{1} \otimes P = \frac{1}{3} \sum_{i,j,r,s=1}^{3} | ir \rangle_A | jr \rangle_B \langle is |_A \langle js |_B . \qquad (C3)$$

This notation fixes the basis in which we will also write $| \psi \rangle$. Indices i, j are used for the first pair and r, s for the second pair.

The minimum of $f(\lambda = 0, \psi)$ is found by requiring the two conditions

a) $\langle\psi|P\otimes P|\psi\rangle = 0$,

b) $\langle\psi|P\otimes\mathbb{1}|\psi\rangle$ maximal .

According to equations (C3) we reach a) only if the entries of either the first or the second pair are orthogonal to each other. We can reach b) if the entries in the first bits of Alice and Bob are identical in both terms of the Schmidt decomposition of $|\psi\rangle$, and if their second bits are in a product state. The coefficient in equation (C2) is easily found to be $|\alpha| = 1/\sqrt{2}$ for maximisation of b).

We can fulfill both conditions a) and b) with the family of states that minimizes f for $\lambda = 0$, denoted by $|\psi^\star\rangle$:

$$|\psi^\star\rangle = \tfrac{1}{\sqrt{2}}(|\,ir\rangle_A|\,is\rangle_B + e^{i\varphi}|\,jr\rangle_A|\,js\rangle_B),\qquad\text{(C4)}$$

with $\langle i\,|j\rangle = 0 = \langle r\,|s\rangle$. Therefore for $\lambda = 0$ we have found the *global* minimum of f to be

$$\min_{\psi} f(\lambda=0) = 0 \ . \qquad\text{(C5)}$$

Using the explicit structure of the states $|\psi^\star\rangle$ we find that

$$\begin{aligned}\langle\psi^\star|\mathbb{1}\otimes\mathbb{1}|\psi^\star\rangle &= 1 \ ,\\ \langle\psi^\star|\mathbb{1}\otimes P|\psi^\star\rangle &= 0 \ ,\\ \langle\psi^\star|P\otimes\mathbb{1}|\psi^\star\rangle &= 2/3 \ .\end{aligned}\qquad\text{(C6)}$$

When varying the parameter λ we therefore find

$$\langle\psi^\star|\rho_2(0\le\lambda\le\tfrac{1}{2})|\psi^\star\rangle = 0 \ . \qquad\text{(C7)}$$

Similarly, for $\tfrac{1}{2}\le\lambda\le 1$ the same line of argument holds when interchanging the role of first and second bits, leading to a different minimizing family $|\psi^\bullet\rangle$. At $\lambda = \tfrac{1}{2}$, the point which is symmetric with respect to interchanging the two pairs, both families lead to the expectation value zero.

In the following we will show that $|\psi^\star\rangle$ corresponds to a local minimum for $0 < \lambda \le \tfrac{1}{2}$.

First, we show that the states given in equation (C4) form a compact set, by describing how to move through the whole family in infinitesimal steps: Looking at the first pair, we can either make the following change:

$$|\,i\rangle \to x_i|\,i\rangle + x_k|\,k\rangle \ \ \text{with} \ \langle k\,|i\rangle = 0 = \langle k\,|j\rangle \ , \qquad\text{(C8)}$$

or we can move to

$$|\,j\rangle \to x_j|\,j\rangle + x_l|\,l\rangle \ \ \text{with} \ \langle l\,|j\rangle = 0 = \langle l\,|i\rangle \ , \qquad\text{(C9)}$$

or we can change both $|\,i\rangle$ and $|\,j\rangle$, keeping $\langle i\,|j\rangle = 0$. Regarding the second pair, we can change

$$|\,r\rangle \to x_r|\,r\rangle + x_p|\,p\rangle \ \ \text{with} \ \langle p\,|r\rangle = 0 = \langle p\,|s\rangle \ , \qquad\text{(C10)}$$

or we can move to

$$|\,s\rangle \to x_s|\,s\rangle + x_t|\,t\rangle \ \ \text{with} \ \langle t\,|r\rangle = 0 = \langle t\,|s\rangle \ . \qquad\text{(C11)}$$

In this way we can move within the family in infinitesimal steps, and there are no isolated points.

Let us now move outside of our family by an infinitesimal amount. We will write down the most general path leading away from the family and then show that first order terms of the expectation value vanish, i.e. we have an extremum, and that the functional determinant of second order terms is positive, i.e. we have a local minimum.

The most general infinitesimal step away from our family is given by

$$|\psi^\star + \delta\rangle = \tfrac{1}{\sqrt{2}}(\sqrt{1+\delta_0}|\,ir\rangle_A|\,(i+\delta_1 k)(s+\delta_2 r)\rangle_B +$$
$$\sqrt{1-\delta_0}\,e^{i\varphi}|\,(j+\delta_3 l)(r+\delta_4 t)\rangle_A|\,(j+\delta_5 m)(s+\delta_6 r)\rangle_B)$$
$$\begin{aligned}\text{with} \quad &\langle k\,|i\rangle = 0 = \langle l\,|j\rangle,\\ &\langle l\,|i\rangle = 0 = \langle t\,|r\rangle,\\ &\langle m\,|j\rangle = 0 = \langle i+\delta_1 k\,|j+\delta_5 m\rangle \ ,\end{aligned}\qquad\text{(C12)}$$

so that the Schmidt terms are still orthogonal, and for each of the seven $\delta_i \ne 0$ we leave the family. Note that we can always keep one state (in this case $|\,ir\rangle_A$) constant by using bilateral rotations.

We now expand the expectation value

$$\langle\varrho_2\rangle = \frac{1}{M^2}\langle\psi^\star + \delta\,|\varrho_2(0<\lambda\le\tfrac{1}{2})|\,\psi^\star + \delta\rangle \qquad\text{(C13)}$$

in powers of δ_i, and find that all terms linear in δ_i are indeed vanishing.

The second order terms can be written down explicitly. The diagonal ones are:

$$\begin{aligned}\mathcal{O}(\delta_0^2): \quad &\tfrac{1}{2}\delta_0^2(1-\lambda) > 0\\ \mathcal{O}(\delta_1^2): \quad &\tfrac{1}{2}\delta_1^2(1+|\,1-2\lambda\,|) > 0\\ \mathcal{O}(\delta_2^2): \quad &\tfrac{1}{2}\delta_2^2(1+|\,1-2\lambda\,|+\tfrac{1}{4}-1) > 0\\ \mathcal{O}(\delta_3^2): \quad &\tfrac{1}{2}\delta_3^2(1+|\,1-2\lambda\,|) > 0\\ \mathcal{O}(\delta_4^2): \quad &\tfrac{1}{2}\delta_4^2(1+|\,1-2\lambda\,|+\tfrac{1}{4}\delta_{ts}-(\lambda\delta_{ts}+1-\lambda)) > 0\\ \mathcal{O}(\delta_5^2): \quad &\tfrac{1}{2}\delta_5^2(1+|\,1-2\lambda\,|) > 0\\ \mathcal{O}(\delta_6^2): \quad &\tfrac{1}{2}\delta_6^2(1+|\,1-2\lambda\,|+\tfrac{1}{4}-1) > 0 \ .\end{aligned}\qquad\text{(C14)}$$

Here δ_{ts} is the Kronecker symbol.

Nearly all off-diagonal terms of second order vanish, the only non-zero one is [note that $\mathcal{O}(\delta_i\delta_j) = \mathcal{O}(\delta_j\delta_i)$]:

$$\mathcal{O}(\delta_2\delta_6): \quad \tfrac{1}{2}\delta_2\delta_6(\lambda-\tfrac{3}{4}) \ . \qquad\text{(C15)}$$

This term is negative for the range $0 < \lambda \le \tfrac{1}{2}$; the corresponding 2x2 determinant, however, is $\det(2,6) = 3\lambda^2 - \tfrac{7}{2}\lambda + 1 \ge 0$ for $0 < \lambda \le 1/2$. Thus we have found the second derivative to be positive, and therefore our family $|\psi^\star\rangle$ corresponds to a local minimum for $0 < \lambda \le \tfrac{1}{2}$. In particular that is the case for $\lambda = \tfrac{1}{2}$, i.e. $\beta = 3/2$ in the

notation of Section IV. It is easy to see that this must also be the case for all $1 \geq \beta \leq 3/2$.

For a complete proof that two copies are not distillable, however, it remains to be shown that this minimum is a *global* minimum for $\beta = 3/2$.

[1] M. Planck, "Über eine Verbesserung der Wienschen Spektralgleichung", *Verhandlungen der Deutschen Physikalischen Gesellschaft* **2**, 202 (1900); "Zur Theorie des Gesetzes der Energieverteilung im Normalspektrum", *ibid.* **2**, 237 (1900).

[2] A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 773 (1996); A. Steane, Rep. Prog. Phys. **61**, 117 (1998); A. Barenco, Contem. Phys.**37**, 375 (1996).

[3] These challenges concern the problem of classification and characterization of positive operator maps on $C^{\star}$–algebras; see for instance E. Strömer, Acta Math. **110**, 233 (1963); S. L. Woronowicz, Rep. Math. Phys. **10**, 165 (1976); M. D. Choi, Lin. Alg. and Its. Appl. **10**, 285 (1975); M. D. Choi, Proc. Sympos. Pure Math **38**, 583 (1982).

[4] An excellent introduction of quantum correlation and entanglement is provided by Peres A, 1995, *Quantum Theory: Concepts and Methods*, (The Netherlands: Kluwer Academic Publishers).

[5] J. S. Bell, Physics **1**, 195 (1964); J. Clauser, M. Horne, A. Shimony, and R. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[6] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[7] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996); V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys.Rev.Lett. **78**, 2275 (1997); V. Vedral and M. Plenio, Phys. Rev. A **57**, 1619 (1998); G. Vidal and R. Tarrach, Phys.Rev. A **59**, 141 (1999).

[8] B. M. Terhal, quant-ph/9911057.

[9] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[10] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Lett. A**223**, 8 (1996).

[11] P. Horodecki, Phys. Lett. A **232**, 333 (1997).

[12] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).

[13] see for instance R. Galindo and P. Pascual, *Quantum Mechanics*, Springer, Berlin, 1993.

[14] A. Sanpera, R. Tarrach, and G. Vidal quant-ph/9707041.

[15] P. Busch and P. Lahti, Found. Phys. Lett. **10**, 113 (1997).

[16] R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A**230**, 377 (1996).

[17] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).

[18] N. J. Cerf, C. Adami, R. M. Gingrich, Phys. Rev. A**60**, 893 (1999).

[19] P. Horodecki, J. A. Smolin, B. M. Terhal, A. V. Thapliyal, quant-ph/9910122.

[20] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys. Rev. A**58**, 883 (1998).

[21] G. Vidal and R. Tarrach, Phys. Rev. A **59**, 141 (1999); see also S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, Phys. Rev. Lett. **83**, 1054 (1999).

[22] M. Lewenstein, A. Sanpera, Phys. Rev. Lett. **80**, 2261, (1998); for recent progress see B. G. Englert and N. Metwally, J. Mod. Opt. **47**, 2213 (2000).

[23] A. Sanpera, R. Tarrach, and G. Vidal, Phys. Rev. A, **58**, 826 (1998).

[24] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999); D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, B. M. Terhal, quant-ph/9908070; C. H. Bennett, D. P. DiVincenzo, Ch. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, W. K. Wootters, quant-ph/9804053; see also R. Horodecki, M. Horodecki, and P. Horodecki, quant-ph/9811004.

[25] B. Terhal, Phys. Lett. A **227**, 319 (2000).

[26] D. Bruß and A. Peres, Phys. Rev. A **61**, 030301(R) (2000).

[27] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein Phys. Rev. A **61**, 062302 (2000) quant-ph/9912010; see also M. Lewenstein, J. I. Cirac, S. Karnas, quant-ph/9903012.

[28] P. Horodecki, M. Lewenstein, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 032310 (2000).

[29] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, quant-ph/0005014.

[30] M. Lewenstein, B. Kraus, P. Horodecki, and J.I. Cirac quant-ph/0005112.

[31] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).

[32] see for instance A. Ekert, Phys. Rev. Lett. **67**, 661 (1991); C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992); C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[33] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996); C. H. Bennett, H. J. Bernstein, S. Popescu and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[34] D. Deutsch, A. Ekert, R. Jozsa, Ch. Macchiavello, S. Popescu and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[35] N. Gisin, Phys. Lett. A **210**, 151 (1996).

[36] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).

[37] It is worth stressing here that the bound entanglement, although nondistillable, may in some situations be activated by combining it with free entanglement in a procedure called quasi–distillation, see P. Horodecki, M. Horodecki and R. Horodecki. Phys. Rev. Lett. **82**, 1056 (1999); the discussion of the problem of quasi–distillabilty of quantum states goes beyond the scope of the present primer.

[38] W. Dür, J. I. Cirac, M. Lewenstein and D. Bruß, Phys. Rev. A **61**, 0262313 (2000).

[39] D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, A. V. Thapliyal, Phys. Rev. A **61**, 0262312 (2000).